IN THE SPECIFICATION

Page 15, replace paragraph 2 with the following amended paragraph:

Fig. 2 is a flowchart illustrating the method of secure communications 200 according to the first embodiment of the invention. The flowchart is organised in columns in the following order: Alice 110, device (A) 120, device (B) 140, and Bob 150. In step 210, Alice 110 speaks a challenge statement C_A, which is input to Device A (shown as device 600 in Fig. 6). Preferably, the challenge statement C_A contains some "freshness" elements, such as the date and time, and news headlines of the day. In step 212, Device A generates a random number x and computes g^x. Device A then preferably computes a key k_A from code g^x using the key generator. Next, Device A encrypts the challenge statement C_A with key k_A using the key generator and sends the ciphertext, referred to as Message A1:

Page 18, replace paragraph 2 with the following amended paragraph:

Fig. 3 is a flowchart illustrating a method of secure communications 300 according to the second embodiment of the invention. In step 310, Alice starts the session by speaking a challenge statement C_A. In step 312, Device A generates a random value x, computes a code g^x and a key k_A from g^x for a symmetric key cryptosystem, encrypts the challenge statement C_A with k_A and sends to B the ciphertext, as Message B1:

$e(k_A, C_A)$.

Page 21, replace paragraph 2 with the following amended paragraph:

Fig. 4 depicts a scenario 400 where Alice attempts to set up a communications

session with Bob and where Clark performs a man-in-the-middle attempt to impersonate Bob to Alice. The flow diagram is accordingly organised into three columns: Alice, Clark and Bob. In step 410, Alice starts a session by generating a random number x, computing g^x, speaking a challenge statement C_A, computing k_A from g^x, encrypting C_A with k_A, and sending the ciphertext $e(k_A, C_A)$ to Bob.